UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information associated with Google Account donspaintingrocks@gmail.com, the cellular telephone number 414-899-6082, or the alternate email address rock2don@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Google, Inc.

Case No. 19-MJ-1249

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. 844(i); 18 U.S.C. 844(m); 18 U.S.C. 1519; 18 U.S.C. 922(a)(6); and 18 U.S.C. 922(d)(9)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Rick Hankins
Applicant's signature

Special Agent Rick Hankins of the ATF
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 6/3/19

William E. Duffin
Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Rick Hankins, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. ("Google") to disclose to the government records and other information, including the contents of communications, associated with the Google Account donspaintingrocks@gmail.com, that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent of the U.S. Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed since April 2003. My duties as a Special Agent with the ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

3. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the ATF National Academy. That training included various legal courses related to constitutional law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as interviewing, surveillance, and evidence collection.

4. In addition to my duties as a criminal investigator, I am also an ATF Certified Fire Investigator (CFI). As an ATF CFI, I am tasked with providing expert opinions as to the origin and cause of fires. I obtained the ATF CFI certification in 2009 following a two-year

training program that centered on various fire science topics including, but not limited to: chemistry, fire dynamics, and building construction. The two-year ATF CFI certification program consisted of college courses, written exams, research papers, reading assignments, practical training exercises, and test burns of various materials. I am re-certified annually as an ATF CFI. Additionally, I have been certified as a fire investigator by the International Association of Arson Investigators since June 2011. I have received over 1,300 class hours of fire-related training.

5. Furthermore, I have been an instructor regarding fire-related topics on 38 occasions for the following agencies and institutions: The National Fire Academy (FEMA), International Association of Arson Investigators Chapter 25, Waukesha County Technical College, and Blackhawk Technical College. I have also participated in over 185 live fire training exercises, where I started training fires and observed fire growth and development. Finally, I was a full-time instructor at the ATF National Academy from approximately August 2015 to August 2016, where I taught several topics during Special Agent Basic Training for new ATF recruits. Specifically, I was a primary instructor for the arson block of training at the ATF Academy.

6. To date, I have participated in over 260 fire scene examinations and have testified as an expert.

7. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

8. As a part of my duties with the ATF, I investigate criminal violations relating to arson and arson-related offenses, including violations of Title 18, United States Code, Section 844. During the course of my investigations, I have regularly participated in the execution of

search warrants involving electronic evidence and regularly used electronic evidence to find evidence of intent, motive, manner, means, and identity.

9. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of the following violations, as described in Attachment B:

a. an arson affecting interstate commerce, in violation of Title 18, United States Code, Section 844(i);

b. conspiracy to commit arson, in violation of Title 18, United States Code, Section 844(m);

c. the destruction, alteration, or falsification of records in federal investigations, in violation of Title 18, United States Code, Section 1519;

d. false statement, in violation of Title 18, United States Code, Section 922(a)(6); and

e. furnishing a firearm to a prohibited person, in violation of Title 18, United States Code, Section 922(d)(9).

10. This affidavit is based upon my personal knowledge as well as information provided to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon information gathered from interviews of citizen witnesses, reports, official records, law enforcement reports, and my training and experience. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

11. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district

court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

12. Google is a United States company that specializes in Internet-related services and products and provides electronic communication services to subscribers. Google provides a variety of products and services that can be accessed from a computing device using a web browser or application ("app").[1]

13. Based on my training and experience, I know that Google offers numerous online-based services, including email (Gmail), an Internet browser (Chrome), search engine (Google), online file storage (including Google Drive and Google Photos), a web mapping service (Google Maps), a calendar (Google Calendar), a GPS navigation software app (Waze), a video-sharing application (YouTube), messaging (Google Hangouts, Google Allo, and Google Messages), and video calling (Google Duo). These products and services can be used on both computers and mobile devices.

14. Google services are accessed through the use of a Google Account. A single Google Account can be linked to multiple Google services and devices, serving as a central authentication and syncing mechanism. Google allow users to create, store, access, share, and synchronize data on any Internet-connected device.

15. An individual can obtain a Google Account by registering with Google. A Google Account takes the form of the full email address submitted by the user to create the account

[1] The information in this section is based on information published by Google on its website.

(often ending in @gmail.com). Additional email addresses can also be associated with a Google Account by the user.

16. Some services, such as Gmail, Google Drive, Google Photos, Google Calendar, Google Hangouts, Google Allo, Google Messages, and Google Duo, require the user to sign in to the service using a Google Account.

17. Other services, such as Chrome, Google, Google Maps, Waze, and YouTube, can be used while signed in to a Google Account, although some aspects of these services can be used even without being signed in to a Google Account.

18. I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternate email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Therefore, Google likely possesses stored electronic communications (including retrieved and unretrieved email for Google users) and information concerning users and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location, or illicit activities.

19. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of

service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

20. **Android:** Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account and users are prompted to add a Google account when they first turn on a new Android device.

21. **Gmail:** In general, I also know that Google typically maintains any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account on its servers unless and until the subscriber deletes the email. Even after deletion, Google may retain those records for a certain period of time.

22. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. Information maintained by the email provider can show how, where, and when the account was accessed or used.

23. Based on my training and experience, I have learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer

Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user's Internet browser.

24. **Google and Chrome:** Google offers a service through which a computer user can search webpages for text that the user enters. Under some circumstances, Google saves the user's text searches to the user's account. For users who enable the feature, Google will maintain Web History, recording information about the user's online activity. Web History records may include, among other things, the Google searches the user conducts, the web sites the user visits, and the videos the user watches. Google's Web and App Activity records for a user may similarly save the user's search activity on applications and browsers, including information about the websites the user visits; the applications that he uses; advertisements that the user clicks; and the user's location, language, and IP address. This activity information can be saved even when the user is offline. Based on my training and experience, I am aware that a user's web and search history may include evidence of the crime itself as well as the user's identity and state of mind.

25. Similarly, Google allows users to save to their account certain data relating to their use of Chrome, Google's web browser, including search history, bookmarks, and other settings. The data is stored on Google's servers and made available to the user wherever Chrome is used, regardless of the device or location. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices. Based on my training and experience, information associated with Chrome may constitute evidence of the crime, as well as indicate the user's identity and location.

26. **Google Drive:** Google Drive is a file storage and synchronization service that allows users to store files in the cloud, synchronize files across devices, and share files with other

users. A user's Google Drive can be accessed from a website and from Windows and macOS computing devices and Android and iOS mobile devices. Google Drive allows a user to store photos, stories, designs, drawings, recordings, videos, and more. Google Drive contains an office suite, including Google Docs, Google Sheets, and Google Slides, which allows collaborative editing. Files created and edited using that office suite are saved in Google Drive.

27. Google Drive also offers a Backups section, which allows a user to backup files from desktop and mobile devices to Google's servers.

28. I know that WhatsApp Messenger, a messaging service owned by Facebook, Inc., allows Android users to backup chats and media to Google Drive.[2] WhatsApp Messenger allows users to send text messages, voice calls, video calls, images, media, documents, and user location. WhatsApp Messenger is accessible from Windows and macOS computing devices and Android and iOS mobile devices.

29. **Google Hangouts:** Google Hangouts is a messaging service that allows users to send messages, video calls, and voice calls. Users can also send photos, videos, maps, and more. These chats can be synced across devices. Hangouts can be used on Android and iOS mobile devices and may be accessed on Internet-connected devices.

30. **Google Allo:** Google Allo was an instant messaging mobile app for Android and iOS mobile devices with a web client for internet browsers, including Chrome. Google

---

[2] The information in this paragraph is based on information published by Google and WhatsApp on their websites, including but not limited to the following webpage: "Backing up to Google Drive," available at https://faq.whatsapp.com/en/android/28000019/.

discontinued Allo in March 2019. The app allowed users to exchange messages, files, voice notes, and images. Google maintained logs of a user's Allo messages indefinitely until deleted by the user.

31. **Google Messages:** Google Messages is a messaging app for Android mobile devices. Messages allows users to send text messages, video calls, images, and media. Messages allows users to sync these messages across devices.

32. **Google Duo:** Google Duo is a high-definition video and audio chat mobile app that can be used on Android and iOS mobile devices and on computing devices using Chrome. Duo also allows users to leave video and voice messages up to 30 seconds.

33. **YouTube:** YouTube is an online service that allows users to share and view videos. Based on my training and experience, I know that Google maintains records for YouTube relating to use (including searches, uploads, deletions, shares, views, edits, comments, and likes), copies of videos and related records (including size, title, description, duration, tags, timestamps, and location information), account information (including user settings, channels, subscriptions, subscribers, and playlists associated with the account, friends and contacts associated with the account, and metadata), and access information (including logs, IP addresses, timestamps, location information, and device identifiers).

34. **Location Information:** Based on my training and experience, I also know that Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google Account, and users are prompted to add a Google Account when they first turn on a new Android device.

35. I also know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

36. I know that cellular devices—including mobile telephones that run the Android operating system and those that do not—are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called "cell sites," which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

37. Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless Internet ("wi-fi") access points if a user enables wi-fi connectivity. Wi-fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

38. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device's transmission range, to which it might connect.

39. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

40. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

41. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system and from devices using Apple's operating system ("iOS") when the user has enabled Google location services. Google then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising.

42. In addition, I know that Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google Account associated with the Android device and/or that is signed in via the relevant Google app. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about wi-fi access points and Bluetooth beacons within range of the mobile device.

43. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or e-mail access.

44. Based on my training and experience, I also known that Google collects and retains information about the user's location if the user has enabled Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol address at the time they engage in certain Internet- and app- based activity and associates this information with the Google Account associated with the Android device and/or that is signed in with the relevant Google app.

45. Google collects location information from Android and iOS mobile devices. This information can derive from GPS data, cell site information, wi-fi access points, Bluetooth, sensor data, user searches, IP geolocation, and other sources. According to Google, location information may be retained and associated with an account when the owner of that account has activated Location Services on a device and has enabled the Location History, Location Reporting, or Web & App Activity settings. This information can be viewed by users on their

Timeline or through on their My Activity dashboard, and is used by Google for business purposes and to enhance user services. Google also utilizes this and other location-related data to enable its advertisers to target advertisements to users with connections to, or interests in, a certain location.

46. Google Maps is an online service that provides users with access to maps, real-time location and traffic information, turn-by-turn directions, and the ability to browse reviews and photos from local businesses. Users can save locations to their account, including home and office addresses and other favorite or commonly-used locations, and utilize "My Maps" to compile and share collections of addresses. Users who allow their Google search activity to be saved to their account will also have their Maps-related search activity saved. Users can share their real-time location with others through Maps by using the Location Sharing feature. Waze is a cross-platform app owned by Google that, like Google Maps, can be used for navigation and allows its users to save locations and share location information with other users. Waze's navigation services are influenced by reports by its users of traffic conditions and related information.

47. Other information may be collected by Google that provides inferences about a user's location. For example, wi-fi access points may have descriptive names or be associated with locations in publicly accessible geolocation databases. IP addresses may also be associated with locations through similar services. Advertising records may contain specific or inferred location information. Metadata associated with image and video files stored by Google on behalf of a user may include information about where the images or videos were taken, such as EXIF data.

48. Location data, such as the location data in Google's possession, can assist in a criminal investigation in various ways. Location data can assist investigators in understanding the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored about the user's account may further indicate the geographic location of the account user at a particular time.

49. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products, as described above, mobile devices that were in a particular geographic area during a particular time frame and to determine which Google Accounts those devices are associated with. Among other things, this information can inculpate or exculpate a Google Account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation.

50. Google will preserve copies of all of the records described above upon receipt of a preservation request pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of these records according to its own data retention policy.

51. In my training and experience, evidence of who was using a Google Account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thereby enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. The stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in

furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

52. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

53. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

54. Other information connected to a Google Account may lead to the discovery of additional evidence. For example, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

II. PROBABLE CAUSE

55. In conjunction with other federal, state, and local law enforcement officers, I am conducting an investigation into an arson affecting interstate commerce and a conspiracy to commit arson that occurred on January 2, 2019 in the vicinity 716 West Rogers Street in Milwaukee, Wisconsin, in violation of Title 18, United States Code, Sections 844(i) and 844(m).

56. On January 2, 2019 at approximately 9:55 p.m., the Milwaukee Fire Department and the Milwaukee Police Department responded to a vehicle fire in the vicinity of 716 West Rogers Street in Milwaukee, Wisconsin. The vehicle was identified as a 2001 Ford F-250 pickup truck bearing Wisconsin license plate MA-9985 and Vehicle Identification Number 1FTNW21L21EC43063. Police officers were informed that the fire was suspicious.

57. A registration check with the Wisconsin Department of Motor Vehicles revealed that the Ford F-250 pickup truck bearing Wisconsin license plate MA-9985 is registered to Matthew Neumann (DOB: XX/XX/1975), who lives at 9426 South 29th Street in Franklin, Wisconsin.

58. At about 11:00 p.m. on January 2, 2019, police officers of the Franklin Police Department contacted Matthew Neumann at his residence. One officer noticed a strong odor of a chemical accelerant, once let inside by Matthew Neumann, and observed clothing lying nearby. Matthew Neumann told the police officers that he owns eight trucks, because he owns a plowing business and that he lets one of his employees drive the Ford F-250 home.

59. Police officers later interviewed Matthew Neumann's family. Tammy Neumann, Matthew Neumann's wife, stated that at approximately 5:00 a.m. on January 2, 2019 she was awoken by Matthew Neumann at their residence at 9426 South 29th Street in Franklin,

Wisconsin. She observed that Matthew Neumann was intoxicated and began undressing, and she also noticed that Matthew Neumann had a black handgun and heard him rack the slide.

60. When she left the house later that morning, Tammy Neumann observed Matthew Neumann's 2001 Ford F-250 pickup truck bearing Wisconsin license plate MA-9985 parked on the driveway and observed a white male, approximately 35 to 40 years old, slumped down in the passenger seat. Tammy Neumann looked through the window and observed no signs of life. She thought that the male had blood around his nose and mouth and that the passenger window may have been spidered, as if struck by a human head.

61. According to Tammy Neumann, Matthew Neumann did not return to the residence until about 10:00 p.m. that night. When he did, Tammy Neumann smelled a strong odor of diesel fuel on Matthew Neumann's clothes, such that she told Matthew Neumann to put the clothes outside.

62. Matthew Neumann's daughter overheard a conversation between Tammy Neumann and Matthew Neumann, where Matthew Neumann said that he shot "Rich" or "Dick" "over a pack of squares." Tammy Neumann and her daughter left the residence and later returned. At that point, the truck was gone along with Matthew Neumann.

63. On January 8 and 11, 2019, I conducted a fire scene examination of the Ford F-250 along with the Milwaukee Police Department and Wisconsin Department of Justice's Division of Criminal Investigation pursuant to a state search warrant. One officer discovered a bullet hole and strike on the B-pillar of the passenger side of the pickup truck, a lead bullet fragment at the base of the B-pillar in the midst of fire debris, and other lead bullet fragments on the B-pillar. Using a trajectory rod, another officer determined that the bullet traveled from the driver seat area to the B-pillar of the passenger seat. Officers also located a bullet and casings

inside of a black melted mass on the driver's side floorboard. I located blood along the weather stripping on the passenger floorboard, removed the passenger seat, and observed additional blood on the flooring and carpeting. I also recovered fire debris from the backseat area that emitted an odor consistent with that of a petroleum distillate.

64. The ATF Forensic Laboratory later analyzed fire debris samples recovered from the truck bed and the backseat area of the Ford F-250. The laboratory results showed the presence of gasoline in the truck bed and back seat area of the Ford F-250.

65. I also obtained surveillance video that captured Matthew Neumann drive the Ford F-250 into the Citgo gas station located at 610 West Becher Street at 9:44 p.m. on January 2, 2019, followed by an early 2000s maroon Chevrolet Impala. Matthew Neumann purchased cigarettes and a lighter at the Citgo gas station. The Ford F-250 and Chevrolet Impala subsequently disappeared east out of the video frame.

66. At approximately 9:47 p.m., a second surveillance video captured the Ford F-250 turn westbound on Rogers Street from South 6th Street, followed by the Chevrolet Impala. The Ford F-250 parked westbound on Rogers Street immediately east of 1978 South 8th Street. The driver's door of the Ford F-250 subsequently opened, Matthew Neumann exited, and a clear illumination appears inside of the Ford F-250 at 9:48 p.m. as the Chevrolet Impala passed. The Chevrolet Impala traveled westbound on Rogers Street and turned southbound on 8th Street, stopping south of the intersection. There was a sudden and intense sustained flash of light inside the Ford F-250 as Matthew Neumann walked and then ran to the parked Chevrolet Impala and entered the passenger side of the Impala. The Impala then drove away. The Impala was captured on surveillance video traveling south on 8th Street away from the burning truck and then west on Becher Street.

67. After examining the Ford F-250, reviewing the surveillance videos, and obtaining laboratory results, I determined that the fire was the result of the human introduction of a heat source to available combustible material inside the passenger compartment of the Ford F-250, including the presence of an ignitable liquid. Based on my knowledge, training, and experience, I conclude this fire was incendiary.

68. Officers also recovered the clothing that Matthew Neumann had been wearing when he returned home on January 2, 2019. That clothing contained the odor of diesel fuel, blood in several areas, and a burn area. That clothing also matched the clothing Matthew Neumann was seen wearing on the Citgo gas station surveillance video minutes prior to the Ford F-250 fire.

69. During an interview with officers on January 10, 2019, Matthew Neumann admitted to starting the fire of the Ford F-250, claiming that he did so accidentally. He claimed that, after the vehicle fire, another vehicle in the area picked him up and that he paid the driver $30 to $40 to take him to a tavern close to his home. Matthew Neumann claimed that the driver of the vehicle was a white male and that the vehicle was burgundy or maroon in color and from the late 1990s or early 2000s—this description is consistent with that of Donald Neumann and Donald Neumann's 2003 Chevrolet Impala.

70. Officers later executed a search warrant on hunting land leased by Matthew Neumann in the Mukwonago area and located a black-and-white Spot Free Cleaning trailer. Next to the trailer was a burn pit containing the heavily charred remains of two individuals, along with other items such as charcoal and charcoal bags.

71. Officers of the Franklin Police Department recovered surveillance video from the Home Depot in Mukwonago, approximately five miles from Matthew Neumann's hunting

property, which depicts Matthew Neumann alone on January 3, 2019 at 10:58 a.m. purchasing four bags of charcoal, lighter fluid, and eight pieces of lumber.

72. According to publicly available court records, the State of Wisconsin charged Matthew Neumann with First-Degree Reckless Homicide, in violation of Wisconsin Statute 940.02, and Mutilating or Hiding a Corpse, in violation of Wisconsin Statute 940.11(2), in Milwaukee County Case No. 2019CF000204.

73. Those records also show that Tammy Lee Neumann is the petitioner in a divorce proceeding against Matthew John Neumann, which was filed on January 22, 2019 in Milwaukee County Case No. 2019FA000372.

74. I have reviewed the cell site and telephone toll records associated with (414) 350-7417, the call number assigned to Matthew Neumann's cellular device. A CLEAR search indicates that DONALD NEUMANN is associated with the call number (414) 899-6082. Detective Jason Ireland of the Franklin Police Department also identified (414) 899-6082, as the cell phone number for DONALD NEUMANN. Detective Ireland has communicated with DONALD NEUMANN multiple times on that call number.

75. The cell site and telephone toll records show that Matthew Neumann's cellphone and Donald Neumann's cellphone exchanged approximately 17 phone calls between 8:02 p.m. and 9:38 p.m. on January 2, 2019. Notably, Matthew Neumann had no other contact with any other number during that time period.

76. The cell site and telephone toll records for Donald Neumann's phone number 414-899-6082 indicate that Donald Neumann's cellphone was in the vicinity of 716 West Rogers Street at about the time of the arson on January 2, 2019, because his cellphone used multiple cell towers and sectors in and around that location. These pings on the cell site maps are also

consistent with Matthew Neumann's cell site and telephone toll records, which indicate multiple calls on or about those times.

77. I know that Donald Neumann has a registered address in the Eastern District of Wisconsin. I have reviewed records from the Wisconsin Department of Transportation, which show that he registered a red 2003 Chevrolet Impala on November 30, 2018 and listed a mailing address of W141N513 Ridgeway Lane in Menomonee Falls, Wisconsin 53051. A CLEAR search also indicates that Donald Neumann registered a red 2003 Chevrolet Impala bearing Wisconsin license plate AEE-6205 on or about November 30, 2018 with a registered mailing address of W141N513 Ridgeway Lane, Menomonee Falls, Wisconsin 53051.

78. On or about January 21, 2019, the Milwaukee Police Department executed a search warrant on Donald Neumann's maroon 2003 Chevrolet Impala. The officers found that the interior of the vehicle had recently been deep cleaned. I compared the photos of Donald Neumann's seized Chevrolet Impala to the surveillance video on the night of the truck fire. There were no dissimilarities in the appearances of the two vehicles. In fact, the color, wheel rims, and trunk spoiler appeared consistent with one another.

79. Samples of the front passenger seat cover of Donald Neumann's Chevrolet Impala were tested and found to contain gasoline.

80. As a result of witness interviews, business records, and search warrant executions, I also know that Matthew Neumann's Ford F-250 was a business vehicle in the name of Spot Free Cleaning and that the Ford F-250 was regularly used in or affecting interstate commerce.

81. Matthew Neumann's address—9426 South 29th Street in Franklin, Wisconsin—and cell phone number 414-350-7417 are also the listed contact information for Spot Free Cleaning Solutions on the publicly available listing on Angie's List

(https://www.angieslist.com/companylist/us/wi/franklin/spot-free-cleaning-solutions-reviews-6459566.htm) (last viewed on January 31, 2019). The description of Spot Free Cleaning on Angie's List is as follows:

> Commercial Cleaning Every masterpiece begins with a crystal clear canvas and the same goes for your business. Whatever your trade, the appearance and cleanliness of your facility are of the utmost importance to customers, employees and the general public. Get your competitive edge at an affordable price with Spot Free Cleaning! When it comes to professionalism and success, it's all about first impressions. With state-of-the-art equipment and over 17 years of commercial cleaning experience, Spot Free guarantees that a first impression will be the last thing on your mind. Sign up for our daily, weekly or monthly cleaning programs to keep your cleaning woes out of sight-out of mind. We offer 24 hour service, 365 days a year! We offer a full range of services including floor care, carpet cleaning, window cleaning, pressure washing and snow plowing. The Spot Free Cleaning difference is simple-we go the extra mile. From the shine of your showroom to a pristine parking lot, you can count on us to get the job done.

82. Matthew Neumann's cell phone number 414-350-7417 is also the listed contact information for Spot Free Cleaning on the publicly available listing on Yelp (https://www.yelp.com/biz/spot-free-cleaning-franklin-2) (last viewed on January 31, 2019).

83. During my fire scene examination, I observed a plow mount on the front end of the Ford F-250, along with a power and control tether for a plow that ran into the passenger compartment of the truck.

84. On January 8, 2019, the Franklin Police Department executed a search warrant at the business address for Spot Free Cleaning. The officers found two work trucks, both with plows attached to their front ends. The photos from that search warrant also show a third plow unattached to a vehicle on the ground. There were no other vehicles at the business location equipped with a plow mount. I believe that the unattached plow found during this search warrant execution had likely been used with the Ford F-250 pickup truck bearing Wisconsin license plate MA-9985.

85. During that search, police officers also recovered business records from Spot Free Cleaning. Those records indicate that Spot Free Cleaning had performed salting and plowing services from at least November 15, 2018 through January 2, 2019. Those records also include contract(s) and addenda between Spot Free Cleaning and Reliable Property Services for a winter snow removal service for the 2018-2019 season. Those documents appear to be signed by Matthew Neumann.

86. On January 29, 2019, police officers from the Franklin Police Department spoke with Tammy Neumann and Matthew Neumann, Jr., who indicated that the Ford F-250 pickup truck was used for business purposes by Spot Free Cleaning, that all employees were allowed to drive and use the Ford F-250 pickup truck for business purposes, and that the Ford F-250 pickup truck was used for snow plowing. Matthew Neumann, Jr. indicated that the Ford F-250 had been used during the winter of 2017-2018, but had not been used during the winter of 2018-2019 because there had not been enough snow.

87. A transaction record from Summit Credit Union shows a business loan in the name of Spot Free Cleaning was issued for a 2001 Ford on or about December 31, 2016, that regular payments have been made since, and that, as of July 20, 2018, a nearly $4,000 balance remained.

88. Insurance documents provided by 1st Auto & Casualty Insurance Company indicates that Matthew Neumann's 2001 Ford F-250 bearing the same Vehicle Identification Number was insured as a business vehicle for Spot Free Cleaning with a policy period of February 18, 2018 to February 18, 2019.

89. During the search of Spot Free Cleaning on January 8, 2019, police officers also recovered approximately 69 firearms from inside of a safe. Many of those firearms still had

evidence tags and zip ties from Matthew Neumann's arrest on November 5, 2015 and related charges in Milwaukee County Case No. 2015CF004844.

90. On January 11, 2019, police officers confiscated another three firearms from a blue trailer on Matthew Neumann's hunting land in Mukwonago. Each of those had previously been confiscated by the Franklin Police Department in 2015.

91. In Milwaukee County Case No. 2015CF004844, Matthew Neumann was found guilty of Endangering Safety by Use of a Dangerous Weapon While Intoxicated (Domestic Abuse), in violation of Wisconsin Statutes 941.20(1)(b) and 968.075(1)(a), and Disorderly Conduct (Domestic Abuse) (Use of a Dangerous Weapon), in violation of Wisconsin Statutes 947.01(1), 968.075(1)(a), and 939.63(1)(a), on January 28, 2016. He was sentenced that day and advised that he was prohibited from possessing a firearm due to his conviction for a crime of domestic violence. (According to publicly available court records, Matthew Neumann is also prohibited from possessing a firearm because he was convicted on or about November 7, 2016 of Fleeing and Eluding, a felony, in violation of Wisconsin Statute 346.04(3), in Milwaukee County Case No. 2016CF003252.)

92. Matthew Neumann, by his attorney, petitioned the court for the return of his firearms. He reached a stipulation with the City of Franklin allowing the release of those firearms to a federal firearms licensee for sale on consignment. In that stipulation, Matthew Neumann, by his attorney, acknowledged that he cannot possess a firearm under federal law and agreed to sell the itemized firearms on consignment. The stipulation and order were issued by the Honorable Janet C. Protasiewicz of the Milwaukee County Circuit Court on November 22, 2016.

93. Matthew Neumann selected Casey W. Steiner, a federal firearms licensee in Franklin, Wisconsin, to sell his firearms on consignment. On or about December 1, 2016, Mr. Steiner took possession of the 64 firearms confiscated from Matthew Neumann.

94. On or about March 18, 2019, I interviewed Casey W. Steiner of Alpha Gunsmith. He provided business records showing that Donald Neumann purchased Matthew Neumann's firearms from Alpha Gunsmith on or about December 2, 2016—the day after their release to Mr. Steiner. Those business records included a Firearms Transaction Record (U.S. Department of Justice and Bureau of Alcohol, Tobacco, Firearms, and Explosives Form 4473) completed by Donald Neumann indicating that he was the actual buyer of the firearms.

95. A law enforcement officer compared the firearms recovered from Matthew Neumann in 2015 with those recovered from Matthew Neumann in 2019 by description and serial number. That comparison revealed that 63 of the 64 firearms confiscated in 2015 and resold were recovered from Matthew Neumann's business and hunting land.

96. On February 1, 2019, this Court issued a search warrant authorizing the search of Donald Neumann's person for the seizure of the cellular device assigned phone number 414-899-6082. On February 4, 2019, I observed Donald Neumann using the cellular device assigned phone number 414-899-6082 in front of his residence, located at W141N513 Ridgeway Lane in Menomonee Falls, Wisconsin 53051. I seized his cellphone—an Apple iPhone.

97. On February 11, 2019, this Court issued a warrant authorizing the forensic examination of Donald Neumann's Apple iPhone.

98. The forensic extraction report indicates that the Apple ID associated with that phone is rock2don@yahoo.com, that an iCloud account is present, and that the MSISDN associated with that phone is 4148996082. The report also indicates that the cellular device was

used to send a text message on February 1, 2019 referring to Donald Neumann's 2003 Chevrolet Impala, stating in substance: "You know my brother has not sat in that car for 10 days Since I picked him up our car has been anywhere and everywhere. Sent this to lawyer too." Officers of the Milwaukee Police Department and Franklin Police Department seized Donald Neumann's 2003 Chevrolet Impala on January 13, 2019—approximately 10 days after the arson on January 2, 2019.

99. A comparison of the forensic extraction report for Donald Neumann's Apple iPhone and the cell site and toll records for Donald Neumann's call number 414-899-6082, the call number assigned to that same cellphone, indicates that relevant electronic evidence immediately prior to the arson was deleted from the cellphone.

100. The forensic extraction report indicates that 76 locations, 24 notes, 87 searched items, and 121 web history items were deleted. The phone's log entries indicate data usage on December 29, 2019, January 2, 2019, January 4, 2019, January 5, 2019, January 7, 2019, January 8, 2019, and January 10, 2019. However, the Chrome search history only dates back to January 3, 2019, the day after the arson. No Chrome search history prior to that date is contained in the forensic extraction report, even though the report indicates numerous Chrome searches after that date until the seizure of the cell phone. Donald Neumann's cell phone also contains records of Safari searches, but only prior to November 19, 2017. There is no search history from November 19, 2017 to January 3, 2019—more than a one-year gap. This suggests that the Chrome search history prior to the arson was deleted.

101. The same is true of call and text message history. The call history contains records of incoming and outgoing phone calls after January 29, 2019. In fact, the forensic extraction report indicates that Donald Neumann made or received 189 calls between January 29,

2019 and February 4, 2019—the date I seized the phone. There are no records of phone calls made using the call number 414-899-6082 prior to January 29, 2019 contained in the forensic extraction report. There are, however, sporadic calls made or received using Facebook Messenger prior to that date.

102. Likewise, the MMS message history only includes messages from January 15, 2019 to January 30, 2019; there are no MMS messages prior to this date. The SMS message history includes messages from January 15, 2019 to February 4, 2019; there are no SMS messages prior to this date.

103. The username rock2don@yahoo.com was first used as a User Account on the cellphone on November 28, 2014, according to the forensic extraction report. The forensic extraction report also indicates that a contact numbers for a "Spoty," a "Tammy Cell", a "Spot," a "Saukville Sue," a "Sherwin Brookfield," a "Sherwin 124th St.," a "Sherwin West Alis," a "Sherwin Grafton," a "Sherwin Pewaukee," and a "Matt & Tammy" contain a timestamp of April 11, 2013. I know that Donald Neumann is a painter by profession. The contact photo for "Matt & Tammy" contains a photograph of Matthew Neumann, and that contact was created on April 11, 2013

104. The forensic extraction report lists Gmail and Chrome as applications installed on Donald Neumann's cellphone. The extraction report also lists donspaintingrocks@gmail.com as a user account on Donald Neumann's cellphone. It contains log entries for gmail.com on dates before and after the arson, suggesting that Donald Neumann used that Google Account from at least September 2016 through February 2019. The extraction report also indicates that www.google.com was regularly accessed by the user of Donald Neumann's cellphone, that

YouTube.com was accessed as early as March 25, 2017, and that Google Maps was regularly used on Donald Neumann's phone to search for locations in January 2019.

105. The web history indicates that the user of Donald Neumann's cellphone used Chrome and Google's search engine in January and February 2019 to search for "smoking gun meaning," "gun dealers franklin wi," news and information related to Matthew Neumann's case, and for attorneys, including the one that petitioned for the release of Matthew Neumann's 64 firearms in 2016.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

106. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

107. Based on the forgoing, I request that the Court issue the proposed search warrant.

108. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Google Account donspaintingrocks@gmail.com, the cellular telephone number 414-899-6082, or the alternate email address rock2don@yahoo.com (the "account") that is stored at premises owned, maintained, controlled, or operated by Google, Inc. ("Google"), a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

Google shall also disclose certain records and information associated with any forwarding or fetching accounts of the account, all other Google Accounts linked to the account because of cookie overlap, all other Google Accounts that list the same SMS phone number as the account, all other Google Accounts that list the same recovery or alternate email address as the account, and all other Google Accounts that share the same creation IP address as the Account.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government, in an unencrypted form whenever available, for each account or identifier listed in Attachment A:

1. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, means and source of payment (including any credit or bank account numbers), and account change history;

2. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized Android and iOS devices and computers, and any devices used to access Google services and products), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses,

Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

3. All records pertaining to devices (including but not limited to Android devices) from which the Account registered or accessed any Google service, to include device serial numbers, model type/number, Device ID, IMEI, MEID, cellular network, phone numbers, MAC addresses, user agent strings, IP addresses, and associated logs and user settings;

4. All records pertaining to the types of service used;

5. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including query logs, mail logs, sign-on logs for all Google services, and logs associated with web-based access of Google services (including all associated identifiers);

6. All search and browsing history associated with the account from November 5, 2015 to present;

7. All Internet search and browsing history, including records associated with Web & App Activity, Web History, and Chrome; the contents of any Chrome data associated with the account, to include bookmarks, passwords, and history; any saved autofill information; and all URLs or IP addresses typed into the Google Chrome address bar or URLs or IP addresses clicked on;

8. All records and information regarding locations where the account or devices associated with the account were accessed with timestamps between November 30, 2016 and December 4, 2016 or with timestamps between December 31, 2018 and January 4, 2019;

9. All location data with timestamps between November 30, 2016 and December 4, 2016 or with timestamps between December 31, 2018 and January 4, 2019, whether derived from data sourced from GPS, cell site information, wi-fi, Bluetooth, sensor data, IP addresses, search history, advertising data, metadata (including EXIF) of images and videos, or any other source.

a. This includes all data associated with Location Services, Location Reporting, Location History, Web & App Activity, and Google's advertising services (including "locations of interest" and other data used by Google for its ad-targeting services) and all information associated with each location record, (including the source, date and time, latitude and longitude, estimated accuracy, device, platform, and inferences drawn from sensor data).

10. All Google Maps and Waze data with timestamps between November 30, 2016 and December 4, 2016 or with timestamps between December 31, 2018 and January 4, 2019, including all saved and starred locations, information associated with search history, locations and other data associated with the use of My Maps and Location Sharing, and the logs and metadata associated with all of the above;

11. The SSIDs and MAC addresses for all wi-fi access points that have been detected by or connected to devices associated with the account with timestamps between November 30,

2016 and December 4, 2016 or with timestamps between December 31, 2018 and January 4, 2019;

12. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken;

13. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google; and

14. Any preserved or backup copies of any of the records or information described above, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

Google is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

15. All records and information described above in Section I that constitutes evidence or instrumentalities of violations involving DONALD NEUMANN or MATTHEW NEUMANN of the following laws of the United States:

a. Title 18, United States Code, Section 844(i) on or about January 2, 2019;
b. Title 18, United States Code, Section 844(m) on or about January 2, 2019;
c. Title 18, United States Code, Section 1519 since on or about January 1, 2019;
d. Title 18, United States Code, Section 922(a)(6) on or about November 5, 2015; or
e. Title 18, United States Code, Section 922(d)(9) on or about November 5, 2015.

This includes records and information relating to the following matters:

a. The identity of the person(s) who created or used the account;

b. How and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crimes under investigation and the account subscriber;

c. The relationship between Donald Neumann and Matthew Neumann;

d. The use, possession, custody, or control of the phone number (414) 350-7417;

e. The use, possession, custody, or control of the phone number (414) 899-6082;

f. Phone numbers associated with Donald Neumann;

g. Phone numbers associated with Matthew Neumann;

h. Email addresses associated with Donald Neumann

i. Land leased by Matthew Neumann located in the vicinity of Mukwonago, Wisconsin;

j. A Home Depot in the vicinity of Mukwonago, Wisconsin;

k. A Citgo gas station located at 610 West Becher Street in Milwaukee, Wisconsin;

l. The knowledge, use, possession, custody, or control of accelerants, ignitable liquids, or heat sources;

m. Donald Neumann's schedule, travel, or location on or about December 1, 2016, December 2, 2016, and January 2, 2019;

n. Matthew Neumann's schedule, travel, or location on or about December 1, 2016, December 2, 2016, and January 2, 2019;

o. *State v. Matthew J. Neumann*, Milwaukee County Case No. 2015CF004844;

p. Casey W. Steiner;

q. Alpha Gunsmith;

r. The transfer or disposition of firearms between Donald Neumann and Matthew Neumann;

s. Firearms recovered from the possession, custody, or control of Matthew Neumann or Spot Free Cleaning in January 2019;

t. Matthew Neumann's purchase, possession, use, transfer, disposition, or discharge of a firearm or firearms from November 5, 2015 to the present;

u. Donald Neumann's purchase, possession, use, transfer, disposition, or discharge of a firearm or firearms from November 5, 2015 to the present;

v. The motive, intent, or knowledge of the violations described above;

w. Preparatory steps taken in furtherance of the violations described above;

x. The concealment or destruction of evidence of the violations described above;

y. The subscriber's state of mind as it relates to the crimes under investigation; and

z. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.